# A Security Based Routing Algorithm and Unique Key Distribution in Wireless Sensor Network

A Santha Devi[#1], Dr. V Vinoba[*2]
[#]*Ph.D., Research Scholar, *Assistant Professor, PG & Research Department of Mathematics, K.N.G.A.College, Thanjavur, Tamil Nadu, India.*

***Abstract***
*A Wireless Sensor Network (WSN) is a kind of remote specially appointed system that sends an expansive number of ease sensor gadgets disseminated over a region of interest. Cooperatively, they report sensor readings to an information accumulation sink or Base Station, routinely or in view of interest. While those with pivoting bunch heads, have likewise favourable circumstances as far as security, the dynamic idea of their correspondence makes most existing security arrangements lacking for them. Grouped sensor systems have been appeared to build framework throughput, diminish framework postponement, and spare vitality. In this research, demonstrate how unique key distribution, generally examined with regards to level systems, can be utilized to secure correspondence in remote sensor arrange. It is insufficient against DoS attack in view of sticking remote channels, or controlling a nodes encompassing condition to prompt the announcing of created conditions. It is the primary work that explores one of a unique key distribution as connected to progressive WSNs.*

**Keywords:** *Security, Unique key distribution, Cluster*

## I. INTRODUCTION

A Wireless sensor systems (WSNs) are developing as an innovation for checking distinctive conditions of interest and they discover applications going from front line observation to natural assurance. At the point when installed in basic applications, WSNs are probably going to be assaulted. Beside the notable vulnerabilities because of remote correspondence, WSNs need physical insurance and are generally conveyed in open, unattended conditions, which makes them helpless against assaults. It is in this manner vital to devise security answers for these systems[5].

A vital issue one needs to handle when utilizing cryptographic techniques to secure a system is key conveyance, which has been seriously contemplated with regards to WSNs. Note, in any case, that an expansive number of WSN designs have been proposed and a key appropriation arrangement that is appropriate to one engineering is likely not to be the best for another, as various system structures display diverse correspondence designs.

Like most routing protocols for WSNs, LEACH is vulnerable to a number of security attacks, including jamming, spoofing, replay, etc. However, because it is a cluster based protocol, relying fundamentally on the cluster heads for data aggregation and routing, attacks involving cluster heads are the most damaging. If an intruder manages to become a cluster head, it can stage attacks such as sinkhole and selective forwarding, thus disrupting the workings of the network. Of course, the intruder may leave the routing alone, and try to inject bogus sensor data into the network, one way or another. A third type of attack is (passive) eavesdropping.

Like most routing conventions for WSNs, LEACH is helpless against various security attacks, including jamming, spoofing, replay, and so forth. Notwithstanding, on the grounds that it is a group based convention, depending in a general sense on the cluster heads for information accumulation and directing, assaults including cluster heads are the most harming. In the event that an interloper manages out how to end up a cluster head, it can organize assaults, for example, sinkhole and particular sending, in this manner upsetting the workings of the system. Obviously, the intruder may allow the directing to sit unbothered, and attempt to infuse false sensor information into the system. A third sort of attack is (inactive) eavesdropping.

In this research, we focus on providing efficient security to pairwise node-to-cluster header communications in LEACH-like protocols. To this end, we first propose security based routing algorithm, a modified version of LEACH that bootstraps its security from unique key distribution. We then give a detailed analysis and performance evaluation of our scheme, and present numbers on how the various parameters impact the trade-offs between cost and security[2].

## II. LITERATURE REVIEW

### *A. A Secure Routing Protocol for Wireless Sensor Networks Considering Secure Data Aggregation*

In this research, the generally unattended and antagonistic arrangements of WSNs and their asset obliged sensor gadgets have prompted an expanding interest for secure vitality productive conventions. Directing and information total get the most consideration since they are among the day by day organize schedules. With the attention to such request, we found that so far there has been no work that lays out a safe directing convention as the establishment for a safe information total convention. The contend that the protected directing part would be rendered futile if the information total plan based on it isn't secure. Then again, the secure information accumulation convention needs a protected fundamental directing convention as its establishment keeping in mind the end goal to be adequately ideal. As an endeavour for the arrangement, we devise an vitality mindful convention in view of LEACH and ESPDA that consolidates secure steering convention and secure information collection convention. We at that point assess its security adequacy what's more, its vitality effectiveness viewpoints, realizing that there are dependably exchange off between both.

### *B. An Authentication Framework for Hierarchical Ad Hoc Sensor Networks*

In this research, Late outcomes demonstrate adaptability issues for level specially appointed systems. To address the issue of adaptability, self-sorting out various leveled impromptu designs are being explored. In this paper, we investigate the assignment of giving information and element verification for various leveled impromptu sensor systems. Our sensor arrange comprises of three levels of gadgets with changing levels of computational and correspondence capacities. Our most reduced level comprises of figure obliged sensors that can't perform open key cryptography. To address this asset limitation, we introduce another sort of endorsement, called a TESLA declaration, that can be utilized by low-controlled hubs to perform element verification. Our system verifies approaching nodes, looks after trust connections amid topology changes through a proficient handoff conspire, and gives information cause validation to sensor information. Further, our structure relegates validation assignments to nodes as indicated by their computational assets, with asset plenteous passages performing computerized marks what's more, keeping up the vast majority of the security parameters. We finish up by giving an underlying execution assessment what's more, security investigation for our system.

### *C. Establishing Pairwise Keys in Distributed Sensor Networks*

In this research, pairwise key foundation is a basic security benefit in sensor systems; it empowers sensor hubs to discuss safely with each other utilizing cryptographic strategies. In any case, because of the asset limitations on sensor hubs, it isn't achievable to utilize customary key administration methods, for example, open key cryptography and key distribution center (KDC). Various key predistribution methods have been proposed for pairwise enter foundation in sensor organizes as of late. To encourage the investigation of novel pairwise key predistribution strategies, this paper builds up a general system for setting up pairwise keys between sensor hubs utilizing bivariate polynomials. This paper at that point proposes two proficient instantiations of the general system: an arbitrary subset task key predistribution plot, and a hypercube-based key predistribution conspire. The examination demonstrates that the two plans have various decent properties, including high likelihood, or assurance to build up pairwise keys, resilience of hub catches, and low stockpiling, correspondence, and calculation overhead. To additionally decrease the calculation at sensor hubs, this paper exhibits an enhancement method for polynomial assessment, which is utilized to process pairwise keys. This paper additionally reports the usage and the execution of the proposed conspires on MICA2 bits running TinyOS, a working framework for arranged sensors. The outcomes show that the proposed systems can be connected effectively in asset compelled sensor systems.

### *D. On the Security of Cluster-Based Communication Protocols for Wireless Sensor Networks*

In this research, Wireless sensor systems are specially appointed systems contained essentially of little sensor hubs with restricted assets, and are quickly rising as an innovation for expansive scale, lowcost, robotized detecting and observing of various situations of intrigue. Bunch based correspondence has been proposed for these systems for different reasons, for example, versatility and vitality proficiency. In this exploration, research the issue of adding security to group based correspondence conventions for homogeneous remote sensor systems comprising of sensor hubs with extremely constrained assets, and propose a security answer for LEACH, a convention where bunches are framed powerfully and intermittently. Our answer utilizes building obstructs from SPINS, a suite of exceedingly improved security building hinders that depend entirely on symmetric-key strategies; is lightweight and jam the center of the first LEACH.

## III. EXISTING SYSTEM

In existing system, Leach accept two kinds of system nodes: an all the more effective Base Station and asset rare sensor nodes. In homogeneous systems with asset rare sensor nodes, nodes don't normally discuss

specifically with the Base Station for two reasons. One, these node commonly have transmitters with constrained transmission run, and can't achieve the Base Station specifically. Two, regardless of whether the Base Station is inside a hub's correspondence extend, coordinate correspondence normally requests a substantially higher vitality utilization. In this manner, hubs that are more remote away for the most part send their messages to middle of the road hubs, which will then forward them to the Base Station in a multi-bounce design.

***Disadvantages***

- The problem with this approach is that, even though peripheral nodes actually save energy, the intermediate nodes, which play the role of routers, end up having a shortened lifetime, when compared with other nodes, since they spend additional energy receiving and transmitting messages.
- A clusters in LEACH are formed dynamically (at random) and periodically, which changes interactions among the nodes and requires that any node needs to be ready to join any cluster head at any time.

## IV. PROPOSED SYSTEM

In proposed Security based routing algorithm used to secure way of data transmission in wireless sensor network. In this research using Unique Key distribution method for security. This key used to secure link between the nodes. Finally, during route-key formation stage, sets of neighboring node that don't share a key can set up their own keys, as long as they are associated by at least two secure connections toward the finish of shared key disclosure. Due to the way keys are allotted, a key can be found in excess of two nodes, and utilized as a part of numerous correspondence joins.

***Advantages***

- Pseudorandom plans make both the unique key distribution and the mutual key revelation more effective.
- High level security management and efficiently.
- An evaluate its security efficiency and its energy-efficiency aspects, knowing that there are always trade-off between both.

## V. METHODOLOGY

### *A. Unique Key Distribution*

The proposed strategy for Unique Key appropriation conspire, every node is allotted out an arrangement of keys drawn from a significantly bigger key pool. Distinctive plans have diverse task calculations, however they all outcome in probabilistic key sharing among the node in the system. A system experiences three stages. In the first stage (unique key distribution), which takes place prior to network organization, a huge pool of *S* keys and their ids are created. Every node is then allocated a ring of *m* keys, drawn from the pool at random, without replacement. In the second stage (distributed-key discovery), which takes place during network setup, all nodes broadcast the ids of the keys on their key rings. Through these broadcasts, a node finds out with which of their neighbors (as determined by communication range) they share a key.

These keys can then be used for establishing secure links between the two neighbors. Finally, during route-key formation stage, sets of neighboring nodes that don't share a key can set up their own keys, as long as they are associated by at least two secure connections toward the finish of shared key disclosure. Due to the way keys are allotted, a key can be found in excess of two node, and utilized as a part of numerous correspondence joins.

At the point when a node is compromised, all its keys are compromised, and every one of the connections secured by these keys are likewise bargained. The underlying task of key rings to nodes should likewise be possible pseudorandomly. Pseudorandom plans make both the unique key distribution and the mutual key revelation more effective.

### *B. Security based Routing Algorithm*

In proposed research, to produce a huge pool of *S* keys and their ids prior to network organization. Each node is then allocated a ring of *m* keys drawn from the pool pseudorandomly, without replacement, as follows. For each node *X*, we use a pseudorandom function to produce its unique id $id_X$. $id_X$ is then used to seed a pseudorandom number generator of a sufficiently extensive period to create a succession of m numbers. RX, the arrangement of key ids doled out to X, would then be able to be acquired by mapping each number in the grouping to its journalist esteem modulus s. Likewise before arrangement, for every node is doled out a pairwise key imparted to the Base Station. The LEACH bunching calculation would then be able to be kept running with the accompanying adjustments: when a self-chose cluster head communicates its adv message, it incorporates the ids of the keys in its key ring; the rest of the node currently group around the nearest cluster head with whom they share a key[5].

In stage 1, a self-chose cluster head *H* communicate its id *idH* and a nonce. In stage 2, standard node Ai process the arrangement of H's key ids (utilizing the pseudorandom plot depicted above), pick the nearest cluster head with whom they share a key k[r], and send it a join req message, ensured by a MAC. The MAC is created utilizing k[r], and incorporates the nonce from H's communicated in Step 1 (to avert replay assaults), and additionally the id r of the key ensured this connection (with the goal that the getting cluster head knows which key to use to check the MAC). In stage 3, the cluster heads send the availability calendar to the node that join their groups, and finish up the first phase. In stage 4, First phase, node to-cluster head interchanges are secured utilizing a similar key used to ensure the join req message in organize 2. An esteem processed from the (nonce) and the detailing cycle (j) is likewise included to counteract replay. In stage 5, The CHs would now be able to unscramble the detecting reports they get, perform information accumulation, and send the total outcome to the Base Station. The total outcome is ensured utilizing the symmetric key shared between the cluster head and the Base Station. For freshness, a counter (shared between the cluster head and the Base Station) is incorporated into the MAC esteem too. In each round j, the estimation of the "freshness token" should be augmented by 1. In fact, the unique key distribution is not helpful for authenticating these broadcasts.

Toward the finish of the grouping procedure, we expect that a small amount of the common nodes will be coordinated with a cluster head, however not really the one they would have coordinated with in the fundamental LEACH, in light of key sharing imperatives; the remaining would not have any cluster head to coordinate with. We call these node vagrants. There are distinctive approaches to manage the vagrants: we can have them rest for the round; we can include a little convention that would permit the "officially embraced kids" to bring the vagrants into their bunches; or we can have them discuss specifically with the Base Station for the round. Regardless, the quantity of vagrants will rely upon the span of the key pool, the measure of the key ring, and the quantity of cluster heads, and will affect the execution of the system.

First phase
1. $H \Rightarrow G$: $id_H$, *nonce,* adv
   $A_i$: choose $r$ such that $r \in (R_H \cap R_{Ai})$
2. $Ai \rightarrow H$: $id_{Ai}$ , $id_H$, $r$, join req, $\text{mac}_{kr}$ ($id_{Ai} \mid id_H \mid r \mid nonce$)
3. $H \Rightarrow G$: $id_H$, (. . . , [$id_{Ai}$, $t_{Ai}$], . . .), sched
Second phase
4. $Ai \rightarrow H$ : $id_{Ai}$ , $id_H$, $d_{Ai}$ , $\text{mac}_{k[r]}$ ($id_{Ai} \mid id_H \mid d_{Ai} \mid nonce + j$)
5. $H \rightarrow$ Base Station : $id_H$, $id_{BS}$,$F$ (. . . , $dAi$, . . .) , $\text{mac}_{kH}$ ($F$ _. . . , $d_{Ai}$, . . .) | $c_H$)
$r$: Id of the keys in the key ring
$R_X$: Set of key ids in node $X$'s key ring
$k_{[r]}$: Symmetric key associated with id
$rj$: Reporting cycle within the current round

## VI. RESULT DISCUSSION

A proposed algorithm is fit for adjusting to meet the validation needs of the sensors coming about because of topology changes. The methodology encourages the foundation of new trust connections as nodes move without requiring the support of the application. This is attractive since it doesn't trouble the application, and henceforth the application does not fill in as a bottleneck. Further, our validation structure does not require the unequivocal investment of the sending nodes in the confirmation of information. We accordingly don't need to refresh any verification parameters because of the versatility of the sending node. The measure of resources required by sensors to store their confirmation keys continues as before as the quantity of sensors increments. Despite the fact that the measure of keys that must be kept up by passages and the application will build, these elements have more assets to commit to security administrations.

### *A. Adaptability*

In experiment result shows that, Energy-efficient and Secure Pattern based Data Aggregation a 60% of energy utilization in this research work. Support Low Energy Adaptive Clustering Hierarchy Algorithm provide a 50% of energy utilization in this research work. A Secure Data Aggregation provide a 40% of energy utilization in this research work. Unique key distribution and security based routing algorithm provide a 70% of energy utilization in this research work. Our proposed unique key distribution and security based routing algorithm provide high adaptability compared with other approach.

**Table 1 Adaptability Analysis**

| Approach | Adaptability |
|---|---|
| Energy-efficient and Secure Pattern based Data Aggregation | 60 |

| | |
|---|---|
| Low-energy adaptive clustering hierarchy | 50 |
| Secure Data Aggregation | 40 |
| Unique key distribution and security based routing algorithm | 70 |

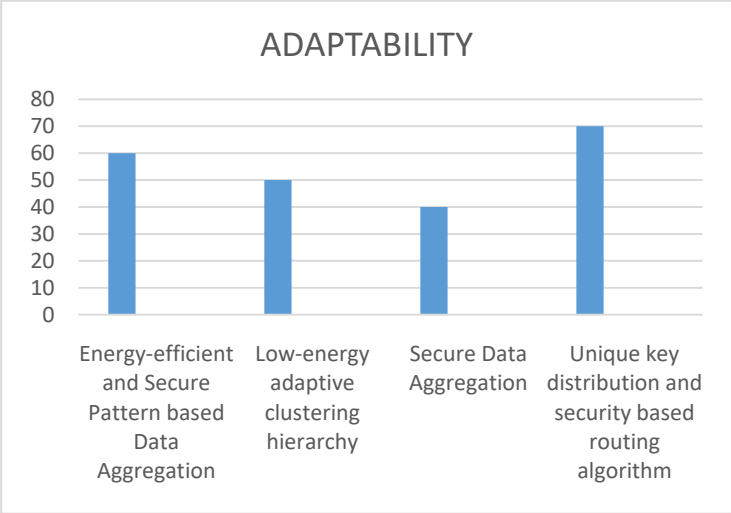


**Fig 1: Adaptability**

***B. Efficiency***

In experiment result shows that, Energy-efficient and Secure Pattern based Data Aggregation a 40% of efficiency in this research work. Support Low Energy Adaptive Clustering Hierarchy Algorithm provide a 50% of efficiency in this research work. A Secure Data Aggregation provide a 60% of efficiency in this research work. Unique key distribution and security based routing algorithm provide a 75% of efficiency in this research work. Our proposed unique key distribution and security based routing algorithm provide high efficiency compared with other approach.

**Table 2: Efficiency Analysis**

| Approach | Efficiency |
|---|---|
| Energy-efficient and Secure Pattern based Data Aggregation | 40 |
| Low-energy adaptive clustering hierarchy | 50 |
| Secure Data Aggregation | 60 |
| Unique key distribution and security based routing algorithm | 75 |

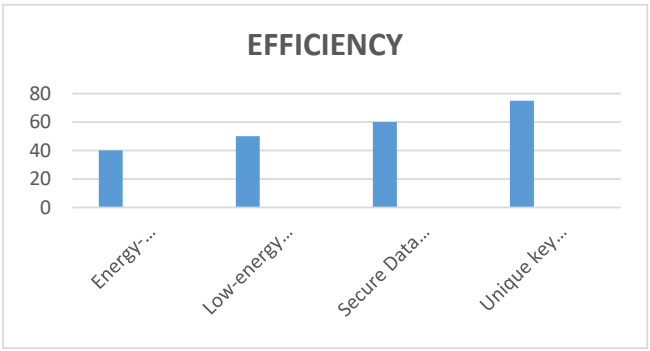


**Fig 2: Efficiency**

***C. Security***

In experiment result shows that, Energy-efficient and Secure Pattern based Data Aggregation a 60% of Security in this research work. Support Low Energy Adaptive Clustering Hierarchy Algorithm provide a 50% of

security in this research work. A Secure Data Aggregation provide a 40% of security in this research work. Unique key distribution and security based routing algorithm provide a 83% of security in this research work. Our proposed unique key distribution and security based routing algorithm provide high security compared with other approach.

**Table 3: Security Analysis**

| Approach | Security |
|---|---|
| Energy-efficient and Secure Pattern based Data Aggregation | 60 |
| Low-energy adaptive clustering hierarchy | 50 |
| Secure Data Aggregation | 40 |
| Unique key distribution and security based routing algorithm | 83 |

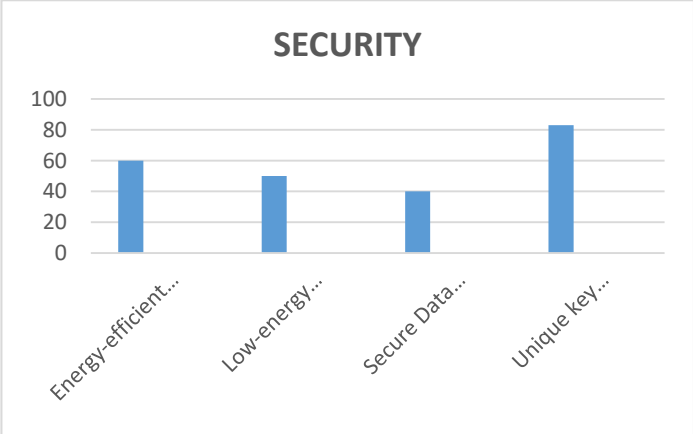


**Fig 3: Security analysis**

## VII. CONCLUSION

In present a security based routing algorithm and unique key distribution, a protocol for securing end-to-end communication in wireless sensor networks. A bootstraps its security from unique key distribution, and can yield different performance numbers on efficiency and security depending on its various parameter values. Our evaluations show that the overhead incurred by security based routing algorithm and unique key distribution is manageable; and memory usage, adaptability, efficiency, and security level can be each traded off for another, dependent on what is most critical in a system.

## REFERENCES

[1] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Security and Privacy (S&P'03), pages 197–213, may 2003.
[2] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili. A pairwise key pre-distribution scheme for wireless sensor networks. ACM Transactions on Information and System Security, 2005. Also appeared in ACM CCS '03.
[3] L. Eschenauer and V. D. Gligor. A key management scheme for distributed sensor networks. In 9th ACM conference on Computer and communications security, pages 41–47, 2002.
[4] D. Estrin, R. Govindan, J. S. Heidemann, and S. Kumar. Next century challenges: Scalable coordination in sensor networks. In Mobile Computing and Networking, pages 263–270, Seattle, WA USA, 1999.
[5] C. Ferreira, M. A. Vilac¸a, L. B. Oliveira, E. Habib, H. C. Wong, and A. A. F. Loureiro. On the security of cluster-based communication protocols for wireless sensor networks. In 4th IEEE International Conference on Networking (ICN'05), volume 3420 of Lecture Notes in Computer Science, pages 449–458, Reunion Island, April 2005.
[6] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In IEEE Hawaii Int. Conf. on System Sciences, pages 4–7, january 2000.
[7] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister. System architecture directions for networked sensors. In int'l Conf. on Architectural support for programming languages and operating systems, pages 93–104, 2000.
[8] J. Hwang and Y. Kim. Revisiting random key predistribution schemes for wireless sensor networks. In 2nd ACM workshop on Security of ad hoc and sensor networks, pages 43–52. ACM Press, 2004.
[9] R. Kannan, L. Ray, and A. Durresi. Efficient key predistribution schemes for sensor networks. In 1st European Workshop on Security in Wireless and Ad-Hoc Sensor Networks (ESAS´04), Heidelberg, Germany, August 2004.
[10] C. Karlof, N. Sastry, and D. Wagner. Tinysec: A link layer security architecture for wireless sensor networks. In 2nd ACM SensSys, pages 162–175, Nov 2004.
[11] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's Ad-Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, 2003. Also appeared in 1st IEEE International Workshop on Sensor Network Protocols and Applications.